

Who is your weakest link?



Session Name: Cyber Security

Session Group: Security, Security, Security

Session Description: This session will provide an overview of Cyber Security within today's organizational or enterprise information technology infrastructure. Time permitting, this session will also have discussion on individual attendee security issues and potential recommendations.

Session Room: Pecos — **Session Presenter:** Gordon Babby, NAS

Session Date: 07/10/2002

Start Time: 1:00 PM — **End Time:** 2:30 PM





Something for everyone?

- ◆ Management
- ◆ Network, System Administrators





Something for everyone?

- ◆ Management
- ◆ Network, System Administrators



- ◆ You ARE kidding, right?



Attributions:

- ◆ portions of the organization and content of this presentation are based upon an excellent white paper (© 12/01) from the work of James P. Cavanaugh of The Consultant Registry. It is a loose constellation of some of the top telecom and security consultants in the US. They may be contacted at...
- ◆ The Consultant Registry www.consultant-registry.com
4405 Northside Parkway, Suite 2120
Atlanta, GA 30327
404-760-0067
info@consultant-registry.com
jcavanaugh@consultant-registry.com
- ◆ **all errors and omissions are entirely from the presenter**



Attributions:

- ◆ portions of the organization and content of this presentation are based upon an excellent comprehensive cyber security text from the work of McClure, Scambray and Kurtz, published by Osborne/McGraw-Hill (© 2001). For more information...
- ◆ Hacking Exposed, Third Edition
2600 Tenth Street
Berkeley, CA 94710
ISBN 0-07-219381-6
- ◆ also, please contact: www.foundstone.com
- ◆ **all errors and omissions are entirely from the presenter**



Managers, Supervisors, Users

Recent surveys show that management...

- ◆ is concerned about security;
- ◆ does not clearly understand the threats, vulnerabilities, risks and liabilities;
- ◆ does not know what to do first in dealing with security problems.

Perhaps they are uncertain about what security actually is?



Cyber Security

a very broad topic about a philosophical concept:
nice, but we don't know what it is! Is it ...

- something you can hold?
- see?
- hear?
- intuit (gut feel)?
- immediately know when it is present?
- immediately know when it is absent?



Said another way...

Security?!?! What IS it?

- an absence of intrusion? of compromise?
- piece of mind?
- resources allocated to even approach these?
- maybe an Unreachable Star?





it's like a special marketplace...



Let's try it on...

- ◆ product – ability for an unauthorized user to compromise networks and systems.
- ◆ currency – time it takes to successfully discover, enumerate and penetrate defenses.
- ◆ willing exchange – will likely occur as long as the currency cost is less than the perceived value of the product.





Possible working definition:

Cyber Security: a state or condition of an enterprise relating to ...

- the visibility and attractiveness of target assets;
- the defenses erected to protect those assets;
- the ability of the organization to notice that its assets are targeted, or attacked;
- the ability of the organization to fend off attacks and quickly recover from them.



Possible objective:

Acceptable cyber security – there's no such thing,
but if an enterprise has ...

- ◆ hidden its assets;
- ◆ added delays (i.e.. defenses);
- ◆ provided security people;
- ◆ continuously monitors and adjusts its programs and policies to stay current;

it likely has an effective, but affordable level of security.



Some lingo...

Assessment – an organized process used by a person or an organization to identify its assets, its threats, its vulnerabilities, its defenses.

Asset – something of value that might be at risk of theft or damage (compromise) by unwanted aggressors.

Attack – the acts of an unwanted aggressor when working to compromise your barriers, or worse, your assets.

Barrier – a defensive mechanism erected by an asset's owner to provide delay.

Breach – the penetration by an unwanted aggressor of a barrier established to protect assets, resulting in intrusion. Unless the attack by the unwanted intruder is immediately interrupted following a breach, a compromise will result.

Compromise – the successful result of the intentional, focused attack of an unwanted aggressor to acquire an asset or to damage a target.

Concealment – a defense put up by an asset's owner to disguise the asset's appearance or to shield its visibility from threats.

Delay – a defense put up by an asset's owner to increase the attack time required for an unwanted aggressor to compromise an asset.



Some more lingo...

Honey Pot – a sacrificial pseudo-asset intentionally presented to unwanted aggressors for the purpose of adding delay by focusing the aggressor on it, rather than on actual assets. Also, this term may connote a “stickiness” element whereby, aspects of the honey pot are designed to trace and identify the aggressor, while (s)he is being entertained by the pot.

Recovery – the process of healing, recovering, restoring order, minimizing damage once you are breached and your asset is compromised.

Target – an asset or set of assets that has been discovered by an unwanted aggressor and identified by him/her/them as an object they intend to compromise.

Threat – a subset of the world population that has been identified in an assessment as a potential group most likely to contain unwanted aggressors that would target your organization or its assets.

Unwanted Aggressor – a person or group from a threat that has targeted an asset for intrusion, compromise or theft.

Unwanted Intruder – an unwanted aggressor that has breached at least one barrier protecting your assets.



Large Enterprise Impediment:

- ◆ In large organizations, such as the US Federal government in general, or in its departments and agencies in particular, personal, individual ownership of security issues is difficult to inculcate.
- ◆ Central Policy Administration weakens
 - rather than strengthens
 - individual resolve to avoid being
 - a weak link.



Thought Food...

- ◆ Do I depend too much on high-level security policy makers to keep our network safe?
- ◆ Do I know how **my** daily work habits fit into the enterprise-wide security posture?
- ◆ How many times a day do I personally think about security aspects of what I am doing?
- ◆ Have I pushed down [to the lowest level possible] the awareness of, application and enforcement of best security practice?

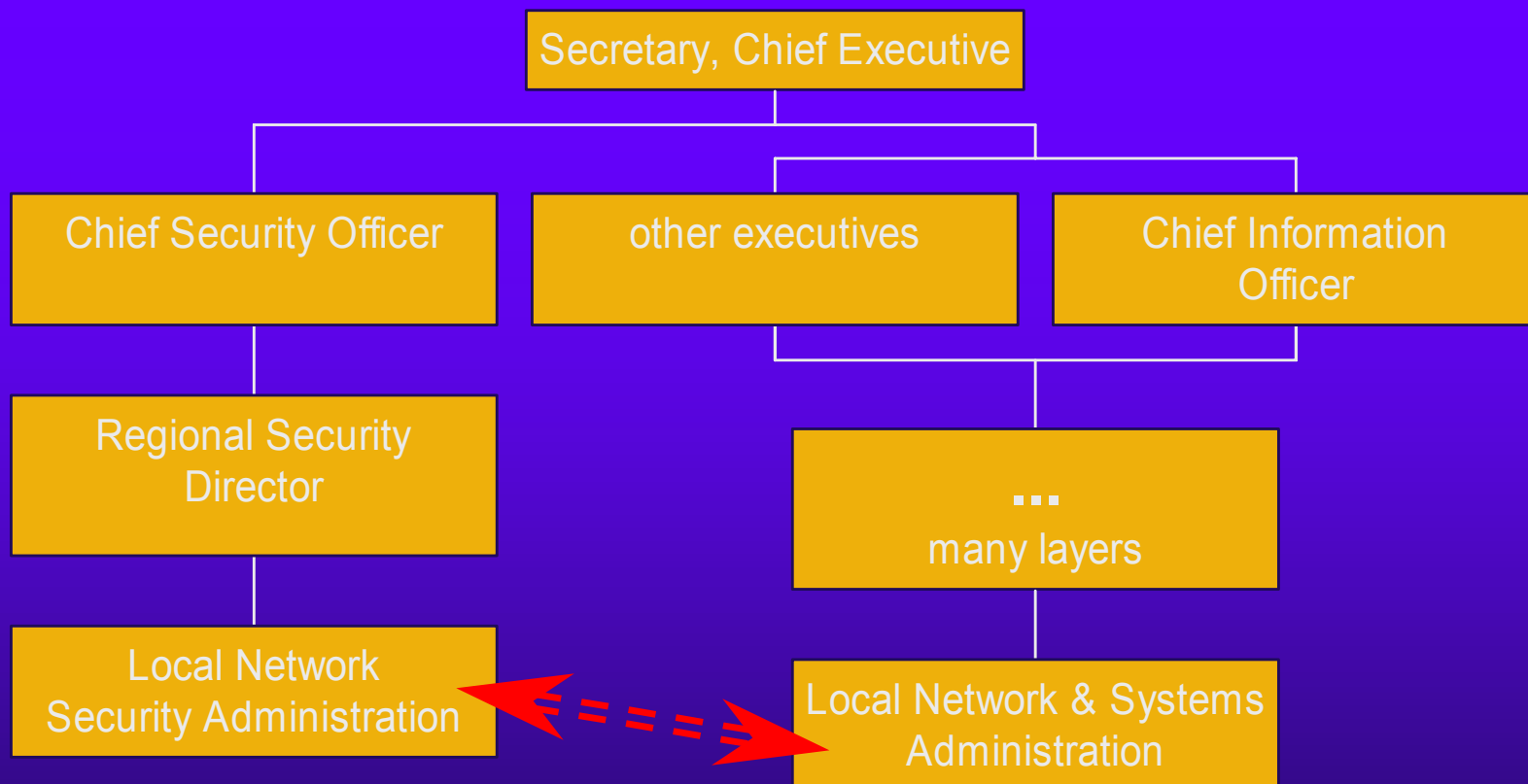


Trends?

- ◆ Is my organization becoming more or less secure?
How do I know?
- ◆ When I leave work each day, do I consider or evaluate my contributions to security?
- ◆ Am I contributing more each day, or less each day to the security posture of my organization?
- ◆ Have I challenged anyone recently?
- ◆ Have I seen anyone challenged recently?



Drifting toward an organization





Six essential queries...

- ◆ **who** wishes to compromise my network?
- ◆ **what** will they likely do? What have they done to others?
- ◆ **why** do they do it?
- ◆ **when** are they likely to strike me?
- ◆ **where** will their attack likely focus?
- ◆ **how** can I know that I am part of a strong defense, not the weakest link?



Who is a threat?

Threat	Avarice	Cyber Criminal	Terrorist	Cracker	Unknown
External					
Crossover					
Internal					



Who is a threat?

Threat	Avarice	Cyber Criminal	Terrorist	Cracker	Unknown
External	5%	3%	2%	5%	5%
Crossover	3%	3%	2%	5%	2%
Internal	20%	15%	5%	15%	15%



Ranking Threats to...

- ◆ Infrastructure -- water, electricity, HVAC, traffic
- ◆ Networks/Phones
 - interruption or DoS voice, data or video services
 - exploitation or theft of telecom service
 - unauthorized disclosure or modification of data
 - unauthorized access to voice, data transmissions
- ◆ Personnel
 - unauthorized facility access
 - personnel safety off site, on travel
 - contamination, cross-contamination of facilities
 - work stoppage
 - threats to personnel, families, contractors, others



Ranking Threats to...

- ◆ Services delivered – interruption, tampering
- ◆ Reputation
 - tampering,
 - unauthorized information compromise or disclosure
 - malicious modification of material (web site)
 - misinformation, incorrect news stories
 - chat room or email based sabotage



Ranking Threats to...

◆ Exploitation of Assets

- theft or relocation of organization assets
- modification of assets, exploitation of agency expertise for criminal gain

◆ Unintentional Aid to Crackers, Terrorists

- providing access to com systems, the internet, wireless to coordinate plans
- providing access to supplies which may be used for terrorism, criminal activity
- providing employment, training, cover



When will I get hit?

- ◆ Holidays
- ◆ Layoffs
- ◆ Acrimonious Employee Separations
- ◆ During Higher Visibility
- ◆ During Lower Security Vigilance
- ◆ Common in Government Sector



Where will I be attacked?

- ◆ at your greatest vulnerability
- ◆ infrastructure
- ◆ network & communications systems
- ◆ personnel
- ◆ service reputation



14 Top Vulnerabilities

1. Inadequate router access control, misconfigured ACLs can allow leakage thru ICMP, IP, NetBIOS leading to unauthorized access to services on your DMZ services.
2. Unsecured and/or unmonitored remote access points provide one of the easiest means of access to your network.



14 Top Vulnerabilities

3. Info leakage can provide cracker with OS and application versions, users, groups, shares, DNS info via zone transfers and running services like SNMP, finger, SMTP, telnet, rusers, rpcinfo, NetBIOS
4. Hosts running unnecessary services e.g.. RPC, FTP, DNS, SMTP are easily compromised.



14 Top Vulnerabilities

5. Weak, easily guessed, and reused passwords at the workstation level can doom your servers to compromise.
6. User or test accounts with excessive privileges.
7. misconfigured internet servers, esp. CGI and ASP scripts on web servers, and anonymous FTP with writable directories.



14 Top Vulnerabilities

8. Software that is unpatched, outdated, vulnerable, or left in default configuration, especially web services.
9. Misconfigured firewall or router ACL can allow access to internal systems directly or once a DMZ is compromised.
10. excessive file and directory access controls (NT shares, UNIX NFS exports).



14 Top Vulnerabilities

11. excessive trust relationships e.g. NT domain trusts, unix .rhosts and hosts.equiv files can provide attackers with unauthorized access to sensitive systems.
12. unauthenticated services like X Windows allow users to capture remote keystrokes.
13. inadequate logging, monitoring and detection capabilities at the network and host level.



14 Top Vulnerabilities

14. lack of accepted and well-promulgated security policies, procedures, standards and guidelines.



Practical Tips...

- ◆ Physical Locks on data, phone closets
- ◆ if possible, arrange for an access control system to throw an alarm to security upon “door ajar”
- ◆ physically inspect closets weekly for suspicious devices (e.g. modems, password recorders)
- ◆ make your log-in account names very different from email address names
- ◆ log-off unattended workstations
- ◆ consider minimizing the removable media devices on workstations



Practical Tips...

- ◆ physical case locks on workstations at least in “public” areas
- ◆ use cracker tools against your network to discover vulnerabilities
- ◆ use security cameras in data centers
- ◆ age passwords rapidly
- ◆ never, ever install anything leaving the default configuration in place



Practical Tips...

- ◆ require at least two different characters
ASCII 033 thru 064 in passwords
- ◆ require both cases in passwords
- ◆ require exactly 7 characters in NT
passwords
- ◆ frequently observe users as they log in to
determine if pwds are written in work areas
- ◆ shadow all passwords



Practical Tips...

- ◆ check your organization's passwords with a cracking tool (see resource list)
- ◆ select and use at least two non-printable ASCII characters for "Administrator" level access e.g.. alt+255 numlock; alt+016 so
- ◆ Rename high access rights accounts like "Administrator," "Back up" using mixed letters, numerals, no "dictionary" words



Practical Tips...

- ◆ audit access to NT's SAM (see resource list)
- ◆ review all of NTBugTraq's Top Ten Security Issues for WinNT (resource list)



Now, let's go forth and secure!!!

I know what ...

- ◆ security is
- ◆ security is not
- ◆ where to focus
- ◆ how to organize
- ◆ resources are here!



Contact Information:

copies of this presentation are available at...

<http://www.nasfed.com/IHS2002.htm>

Bob Townsend, Chief Technology Officer

Paul Norman, Dir., Technical Services

5400 S. Syracuse Street

Greenwood Village, CO 80111

303-799-6077

www.nasfed.com

